generating means for generating a program portion for sending to the source of the access request,

wherein after access to the program portion is permitted and said program portion is operable, in use:

to generate a request for access to the cryptographically protected data set;

on receipt of the cryptographically protected data set, to convert it into an unprotected form; and

to restrict or prevent access to copy or save functions in respect of the data set when in said unprotected form.

30. (New) A method of protecting data downloaded from a server computer to a client computer, said method comprising:

downloading a protected copy of requested data from a server to a client; and

running a program at the client after access to the program is permitted to both: (a) unprotect the downloaded data thereby to provide access to an unprotected copy of the requested data, and (b) restrict or prevent client computer copy and save functions with respect to the unprotected copy of the requested data.

REMARKS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 1-8, 12, 14-18, 21-26 and 28-33 are pending in this application.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current Amendment. The attached is captioned "**Version With Markings to Show Changes Made**."

Rejections Under 35 U.S.C. §103:

Claims 1-8, 12, 14-18, 21-26 and 28-30 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Yourdon, in view of Dean et al (hereinafter "Dean"), Wobber et al (U.S. '642, hereinafter "Wobber") and further in view of Richardson (PCT '204). Applicant respectfully traverses this rejection.

The Office Action states the following:

> "Applicants' arguments received on 6/20/2000 have been fully considered but they are not persuasive with previous cited references for 35 U.S.C. §103(a) rejections. All the answers to the arguments on pp. 10-13 of the amendment received on 6/20/2000 are within court case decisions that the examiner submits as followings:..."

The Office Action then lists several court cases including quotations and/or caselaw citations. However, the Office Action fails to indicate any specific applications of these broad quotations and/or caselaw citations to the specific prior art and claimed invention at issue in the present application. Applicant therefore respectfully requests that if the rejection over Yourdon, Dean, Wobber and Richardson is maintained, Applicant respectfully requests that the next Office Action describe in detail how the broad quotations and/or caselaw citations apply specifically to these prior art references and the claimed invention so that Applicant can obtain a clearer understanding of the rejection and develop an appropriate response thereto.

In order to establish a prima facie case of obviousness, all of the claimed limitations must be taught or suggested by the prior art and there must be some

suggestion, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings.

The Office Action admits that Yourdon and Dean "do not directly address the specific problem of protecting from copying data, & authentication which have been downloaded from a server to a client, nor its solution as in claim 1." (See page 6 of the Office Action.) Applicant submits that Wobber fails to remedy this deficiency of Yourdon and Dean. Wobber is concerned with the problem of authenticating the source of requests for access to data in a distributed information system. Applicant submits that all of the security measures to control access by a requestor to data is implemented at a server, not a program portion running on a client. Wobber further fails to teach or suggest selectively controlling access to copy or save functions at the client in respect of unprotected data once access has been granted by the server. Accordingly, Applicant respectfully submits that even if Yourdon, Dean and Wobber were combined as proposed by the Office Action, the combination would not have taught or suggested all of the claimed limitations of independent claims 1, 28 and 30. With respect to independent claim 22, the combination fails to teach or suggest, inter alia, "downloading data encrypted by means of the cryptographic key to the identified client using the key from the unique determinator."

With respect to Yourdon, Yourdon discloses a conventional password protection technique in which a password is used to determine an end user's authorization to invoke certain functionality or to access certain data. Yourdon, however, does not explicitly state whether the password protection scheme disclosed

therein is implemented in respect of functionality or data residing at a server or that available at a client. If anything, since Yourdon states, "As long as I can control the security of my own server, then I can control the environment of the client platform, too (emphasis added)," immediately before the statement "The most likely scenario for the typical client-server application is one in which the application asks for a password, when appropriate, to determine the end-user's authorization to invoke certain functionality or access certain data," Applicant submits that Yourdon discloses the security of access to applets stored at a server. In summary, Yourdon fails to therefore discuss password protection for a client-server arrangement in the context of functionality and data residing at a client. Again, Yourdon merely discusses password protection for a client-server arrangement in context of functionality and data residing at a server.

Moreover, claim 1 requires "after the running of the program portion has begun and under control of the program portion at the client, converting the cryptographically protected data to an unprotected form and selectively controlling access to copy or save functions at the client in respect of the data in its unprotected form (emphasis added)." That is, the present invention enables access to copy or save functions to be selectively controlled after running of the program portion has begun. In contrast, conventional password protection (such as that disclosed by Yourdon) prevents the running of an access-restricted program from even beginning (if, e.g., unauthorized password is provided beforehand). That is, an access-restricted program cannot be run if a password protection scheme is not first successful passed (via an authorized password) under conventional a password protection scheme.

The Office Action notes that Yourdon states "the application will interact with the browser to encrypt/decrypt transmission between the client and the server." However, this reference to transmissions between a client in a server is an entirely conventional technique for protecting data in transit. There is no suggestion by Yourdon that the functionality available at a client is in any way linked to the encrypted/decrypted status of data residing at the client.

As also noted by the Office Action, Yourdon states that "Development tools must therefore help create secure access to functionality and data, as well as secure transmission of confidential data across the Internet." This objective, however, is common to many security arrangements, but says nothing on how the "development tools" achieve this objective in the context of application programs or data.

As noted by the Office Action, Yourdon discusses that Microsoft has contemplated adding "digital signatures" to applets so that a user downloading an applet may be sure of its source and origin. However, digital signatures and other forms of identification such as "digital watermarking" are not a form of cryptographic protection in that they do not in themselves protect or prevent access to data. In contrast, the present invention is concerned primarily with what can be done with unprotected data at a client. Moreover, independent claims 1, 28 and 30 require converting protected data to unprotected data at the client. Digital signatures are not applied to data so that they can be removed at the client. The digital signature remains embedded in data permanently so that the origin of the data may be determined in any future copy.

Dean discusses security issues relating to Java applets. Specifically, Dean is concerned with features of a Java sub-system in a web browser environment that an applet may gain access to by bypassing security arrangements. As noted by the Office Action, Dean states, "In Netscape Java applets can name only those functions and variables explicitly exported to the Java sub-system." Applicant submits that this passage of Dean refers to functions and variables of the Netscape browser environment exported to the Java sub-system interfacing to Netscape. This is not a feature under the control of a Java applet and is therefore does not teach or suggest copying or saving functions at a client in respect of data in its unprotected form.

Richardson is only discussed briefly with respect to dependent claims 5, 6 and 17. Applicant respectfully submits that Richardson fails to remedy any of the deficiencies of the combination of Yourdon, Dean and Wobber discussed above.

Accordingly, Applicant respectfully submits that claims 1-8, 12, 14-18, 21-26 and 28-30 are not obvious over Yourdon, Dean, Wobber and Richardson and respectfully requests that the rejection of these claims under 35 U.S.C. §103 be withdrawn.

New Claims:

New claims 31-33 have been added to provide additional protection for the invention. Claim 31 includes, inter alia, restricting or preventing access to copy or save functions at the client in respect of the data in its unprotected form. Independent claim 32 requires, inter alia, "to restrict or prevent access to copy or save functions in respect of the data set when in said unprotected form" and independent claim 33 requires "running a program at the client to...(b) restrict or prevent client computer

copy and save functions with respect to the unprotected copy of the requested data."

The cited prior art is not believed to teach or suggest such limitations.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

Raymond Y. Mah
Reg. No. 41,426

RYM:sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

VERSION WITH MARKINGS TO SHOW CHANGES MADE IN THE CLAIMS:

1. (Twice Amended) A method of protecting data sent from a server to a client, said method comprising:

running a program portion at the client, the program portion generating and uploading to the server a request for access to data;

cryptographically protecting the data;

sending the cryptographically protected data to the client; and

after the running of the program portion has begun and under control of the program portion at the client, converting the cryptographically protected data to an unprotected form and selectively controlling access to copy or save functions at the client in respect of the data in its unprotected [at] form.

28. (Amended) A server for providing access to data sets in a protected form, the server comprising:

an input for receiving a request for access to a data set;

protecting means for cryptographically protecting the requested data set; and

generating means for generating a program portion for sending to the source of the access request,

wherein said program portion is operable and after the program portion is permitted to run at the source of the access request, in use:

to generate a request for access to the cryptographically protected data set;

on receipt of the cryptographically protected data set, to convert it into an unprotected form; and

to selectively control access to copy or save functions in respect of the data set when in said unprotected form.

30. (Amended) A method of protecting data downloaded from a server computer to a client computer, said method comprising:

downloading a protected copy of requested data from a server to a client; and

running a program at the client so that after running the program at the client has begun at the client, the program serves to both: (a) unprotect the downloaded data thereby to provide access to an unprotected copy of the requested data, and (b) suppress client computer copy and save functions with respect to the unprotected copy of the requested data.